

REMARKS

Applicants thank the Examiner for the telephonic interview accorded to applicants' prior representatives from the law firm of Fish & Richardson on December 12, 2005. Applicants request reconsideration in light of the foregoing amendments and the following remarks.

Claims 1-11 were examined and are rejected.

Independent claims 1 and 7 are hereby amended. Claims 12-15 are hereby added. All claim changes and additions are supported by applicants' originally-filed application.

Applicants note that a Preliminary Amendment was filed with the originally filed application, which Preliminary Amendment amended claim 3 to delete the multiple claim dependency. However, claim 3 as set forth in prior responses was written in its original un-amended form. Claim 3 included in the foregoing claim listing with this Response reflects the language of claim 3 as amended by that Preliminary Amendment and has a "Previously Presented" legend.

35 U.S.C. §102 REJECTIONS

Claims 1-3 and 7-11 are rejected under 35 U.S.C. §102(e) over Morar et al. [USP 6,678,822; "Morar"]. Applicants traverse.

Amended claim 1 recites a method for encrypting characters from a data element in a database. The method includes reading information identifying a data type associated with data in a particular column of the database from a location in the data base, the location being outside the particular column, and reading a data element from the particular column where the data element includes a first character string. The method also includes forming a restricting character set on the basis of the data type, and encrypting the first character string into a second character string where each character in the second character string is selected from the

restricting character set.

In contrast, Morar does not teach or suggest at least that the data type is read from the database. Instead, in Morar, the data type is deduced based on an analysis of the string being processed when creating the obscured information container. For at least for this reason, Morar is distinguishable from amended claim 1.

The entire discussion in Morar is directed to communicating data from a first processing system in a trusted environment to a second processing system, where the second processing system and/or the communications link between the two processing systems is considered to be an un-trusted environment. Because of the concern with protecting private information found in information containers accessible by the first processing system when in the *un-trusted* environment, Morar describes protecting such private information by creating an information container in which the private information is obscured. In this way, the private information cannot be accessed while it is in an *un-trusted* environment.

Morar does not teach or suggest anything about retrieving the information to be transmitted from a database of the first processing system or how the transmitted information is to be saved in a database once received at the second processing system. Morar is concerned mostly with the further processing or analysis of the transmitted information packet by the second processing system, when the second processing system forms an *un-trusted* environment.

Other than the part of col. 12 directed to email communication, Morar is directed to the creation of an obscured information container that is transmitted electronically via the a communications network such as the Internet or via a recordable medium (*e.g.*, a floppy disk) that would be inserted into a reading device accessible by the second processing system. While the obscure information container is being created and transmitted in Morar, there is no description that this container is being saved in a database for later retrieval at the first processing system or what happens to this information container when it is received at the second processing system. In fact, for the processing examples given in Morar, the information container is

described as being processed separate and independent of other information containers. For example, an information container that is being sent to the second processing system to determine if it is infected with a virus is going to be isolated from other information at the second processing system to prevent the spread of the infection.

As for the part of Morar regarding email transmissions, it is clear that when the mail arrives at the destination the attached file is unencrypted thereby un-obscuring the obscured information in the attached file. There is no further discussion, however, as to what happens to the mail after it is unencrypted.

In sum, it is clear that Morar is limited to communicating information between processing sites in which the receiving site and/or the communication's pathway(s) is an un-trusted environment, and to preventing the disclosure of private information when the receiving site is an un-trusted environment. Morar does not anywhere teach or suggest the storage of information in a database.

Applicants submit that the foregoing remarks distinguishing amended claim 1 from Morar also apply to distinguish from Morar the system recited in amended claim 7. Claims 2-6 and 8-11 depend directly or indirectly from amended claim 1 or amended claim 7, and thus claims 2-6 and 8-11 also are patentable over Morar.

35 U.S.C. §103 REJECTIONS

Claims 4-6 are rejected under 35 U.S.C. §103. Claims 4 and 6 are rejected over Morar in view of Schneier ("Applied Cryptography"), and claim 5 is rejected over Morar in view of Schneier and further in view of Marshall et al. [USP 4,866,707; "Marshall"]. Applicants traverse.

Each of claims 4-6 depends directly or indirectly from amended claim 1. As indicated above, Morar does not teach or suggest the method recited in amended claim 1. Neither Schneier

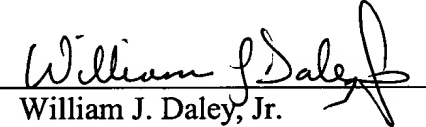
Applicants: Ulf Mattsson et al.
U.S.S.N.: 09/721,942
Response to Office Action
Page 10 of 10

nor Marshall provides at least what Morar lacks, and thus no combination of these references could or would have resulted in the method recited in amended claim 1. Claims 4-6 are patentable for at least this reason.

Although new claims 12-15 have been added to this application, applicants believe that an additional claims fee is not required. However, if for any reason such a fee is required, please charge our Deposit Account No. **04-1105**.

Respectfully submitted,
Edwards Angell Palmer & Dodge, LLP

Date: August 30, 2006

By: 
William J. Daley, Jr.
(Reg. No. 35,487)
P.O. Box 55874
Boston, MA 02205
(617) 439- 4444

Customer No. 21,874

Bos2_556508